Document Number 1

Entry 1 of 1 File: USPT Feb 2, 1999

DOCUMENT-IDENTIFIER: US 5867666 A
TITLE: Virtual interfaces with dynamic binding

DEPR:
At a step 252, the router 120 wraps the packet 200 in a LEX protocol wrapper 210, comprising a LEX header 211 and a LEX body 212. The LEX protocol is the protocol used by the router 120 for communication with the network extender 110 using the communication link 123. The LEX body 212 comprises either a sequence of data for the network extender 110 to redistribute onto the network 101 (that is, a network packet 200), or may comprise a control message designated for the network extender 110 itself.

DEPR:
At a step 256, the network extender 110 unwraps the LEX header 211 from the LEX protocol wrapper 210, and redistributes the LEX body 212 as a network packet 200 onto the network 101 using the network interface 104. The network's communication medium 102 transmits the network packet 200 to its destination device 103 (or devices 103, for example if the network packet 200 is a broadcast packet).

DEPR:
At a step 268, the network extender 110 wraps the network packet 200 in the LEX protocol wrapper 210, comprising a LEX header 211 and a LEX body 212, and transmits the LEX protocol wrapper 210 to the router 120 using the communication link 123. The LEX body 212 comprises the network packet 200.

DEPR:
At a step 269, the router 120 unwraps the LEX header 211 from the LEX protocol wrapper 210. The router 120 compares the LEX body 212 against an access list or a filter list to determine if the LEX body 212 should be forwarded to the second network 124. If so, the router 120 redistributes the LEX body 212 as a network packet 200 onto the second network 124, and the second network 124 transmits the network packet 200 to its destination device 103 (or devices 103, for example if the network packet 200 is a broadcast packet). Otherwise, the router 120 discards the LEX body 212.

Document Number 1

Entry 1 of 1 File: USPT Oct 26, 1999

DOCUMENT-IDENTIFIER: US 5974452 A
TITLE: Process for determining a target ATM address

DEPR:
The return of an address resolution response is especially beneficially configured when the address resolution request LE.sub.-- ARP Request has the E.164 address of the customer premises equipment CPE of the output ELAN ELAN1 attached to it upon encapsulation by the interworking function, when, upon de-encapsulation of the address resolution request, the output E.164 address of the address resolution request is stored in the customer premises equipment CPE of the ELAN2, and this output E.164 address, upon encapsulation of the address resolution response handed over by the LAN emulation server LES of the ELAN2 to the customer premises equipment CPE of the ELAN2 via the access LEG LEC Z2, is attached to the header part of the packet to be transmitted via the network CLSnet offering a connectionless service. As a result thereof, an immediate transmission of the address resolution response LE.sub.-- ARP Response in encapsulated form to the customer premises equipment CPE of the ELANI is enabled by the network CLSnet offering a connectionless service.

CPE

Document Number 1

Entry 1 of 4 File: USPT Oct 26, 1999

DOCUMENT-IDENTIFIER: US 5974452 A
TITLE: Process for determining a target ATM address

DEPR:
The return of an address resolution response is especially beneficially configured when the address resolution request LE.sub.-- ARP Request has the E.164 address of the customer premises equipment CPE of the output ELAN ELAN1 attached to it upon encapsulation by the interworking function, when, upon de-encapsulation of the address resolution request, the output E.164 address of the address resolution request is stored in the customer premises equipment CPE of the ELAN2, and this output E.164 address, upon encapsulation of the address resolution response handed over by the LAN emulation server LES of the ELAN2 to the customer premises equipment CPE of the ELAN2 via the access LEG LEC Z2, is attached to the header part of the packet to be transmitted via the network CLSnet offering a connectionless service. As a result thereof, an immediate transmission of the address resolution response LE.sub.-- ARP Response in encapsulated form to the customer premises equipment CPE of the ELANI is enabled by the network CLSnet offering a connectionless service.

Document Number 2

Entry 2 of 4 File: USPT Feb 2, 1999

DOCUMENT-IDENTIFIER: US 5867666 A
TITLE: Virtual interfaces with dynamic binding

DEPR:
At a step 269, the router 120 unwraps the LEX header 211 from the LEX protocol wrapper 210. The router 120 compares the LEX body 212 against an access list or a filter list to determine if the LEX body 212 should be forwarded to the second network 124. If so, the router 120 redistributes the LEX body 212 as a network packet 200 onto the second network 124, and the second network 124 transmits the network packet 200 to its destination device 103 (or devices 103, for example if the network packet 200 is a broadcast packet). Otherwise, the router 120 discards the LEX body 212.

Document Number 1

Entry 1 of 1 File: USPT Feb 2, 1999

DOCUMENT-IDENTIFIER: US 5867666 A
TITLE: Virtual interfaces with dynamic binding

DEPR:
The network 101 comprises a network extender 110 coupled to the communication medium 102 using a network interface 104. The network extender 110 comprises a special purpose processor or a general purpose processor operating under control of a program memory, and a data storage memory, and is disposed for connectivity to the network 101 using the network interface 104.

DEPR:
In a preferred embodiment, the network extender 110 comprises one of the "C1000 LAN Extender" products, available from cisco Systems, Inc., of San Jose, Calif., and is disposed to be configured for connectivity to an ethernet LAN or a token ring LAN.

DEPR:
The network extender 110 is also coupled to a serial port 111, and is disposed for controlling the serial port 111 according to a known serial port protocol, preferably a point-to-point protocol like that described with FIG. 2. The serial port 111 is disposed for coupling to a serial communication link 112, such as a telephone line coupled to a telephone network 113 or other network.

DEPR:
The virtual port 135 provides the application 131 with the same interface as if the router 120 were coupled directly to the network 101 using a directly connected network interface 104. Accordingly, there is one type of virtual controller 134 for each type of network interface 104 to which the router 120 is disposed for coupling. In a preferred embodiment, the virtual controller 134 is configured for ethernet LANs operating according to an ethernet protocol. When a communication link 123 is established between a network extender 110 and the router 120, the router's operating system selects the virtual controller 134 matching the network extender 110 and its network 101 for coupling to the physical controller 132.

DEPR:
In a preferred embodiment, the serial port 121 is disposed for dynamic binding to one of a plurality of serial ports 111, by sequentially making and breaking the communication link 123 between the router 120 and one of a plurality of network extenders 110. The plurality of network extenders 110 are preferably each coupled to a different network 101, so dynamic binding of the serial port 121 allows the router 120 to sequentially couple to one of a plurality of networks 101.

DEPR:
In a preferred embodiment, an operator sets up an initial configuration for the virtual controller 134, indicating which virtual controller 134 should be bound to which network extender 110, preferably matching the MAC address of the network extender 110 to the initial configuration for the virtual controller 134, such as an

initial configuration for an ethernet LAN operating using an ethernet LAN protocol. The router's operating system creates one software instantiation of the virtual controller 134 for each matching network extender 110 to be coupled to the router 120. This allows each software instantiation of the virtual controller 134 to dispense with switching context when the communication link 123 is made or broken. Multiple software instantiations are known in the art of computer operating systems.

DEPR:
Each instantiation of the virtual controller 134 also maintains state information about the emulated port 133 and the first network 101, in a status record 136, as if the communication link 123 between the network extender's serial port 111 and the router's serial port 121 were continually coupled. Information in the status record 136 is maintained persistently across multiple sessions of the communication link 123. This information includes authentication/identification data 137 for the communication link 123, such as a unique identifier for the network extender 110. In a preferred embodiment, the authentication/identification data 137 comprises the MAC address for the device embodying the network extender 110 and is received from the network extender 110 when the communication link 123 is established.

DEPR:
In alternative embodiments, the authentication/identification data 137 may comprise different or additional information. For example, the authentication/identification data 137 may comprise an identifying serial number for the network extender 110. The authentication/identification data 137 may also comprise information for a more elaborate or secure method of authentication, such as a password.

DEPR:
In a preferred embodiment, the application 131 is disposed to supply administrative services to the network 101 when the router 120 is coupled to the network extender 110. The application 131 supplies administrative control packets 140 to the virtual controller 134, which couples them to the emulated port 133 and the physical controller 132, which couples them to the serial port 121 and the serial link 122, which couples them using the communication link 123 to the serial link 112 and the serial port 111 at the network extender 110, which couples them to the network 101, all using a point-to-point protocol described with FIG. 2. On the network 101, the network extender 110 receives the administrative control packet 140 and processes it accordingly to effect a network administrative service.

DEPR:
In general, the physical controller 132 may comprise any form of connection between the router 120 and the network extender 110, or more generally, any form of connection between two devices, such as a serial port and a serial port controller, a PCMCIA port and a PCMCIA port controller, a computer backplane, or another form of connection. The virtual controller 134 may comprise any interface to the physical controller 132, such as an ethernet interface, a token ring interface, a PCMCIA interface, or another form of interface, and need not be constrained by the physical nature of the connection.

DEPR:
At a step 252, the router 120 wraps the packet 200 in a LEX protocol wrapper 210, comprising a LEX header 211 and a LEX body 212. The LEX protocol is the protocol used by the router 120 for communication with the network extender 110 using the communication link 123. The LEX body 212 comprises either a sequence of data for the network extender 110 to redistribute onto the network 101 (that is, a network packet 200), or may comprise a control message designated for the network extender 110 itself.

DEPR:
At a step 253, the router 120 transmits the LEX protocol wrapper 210 to the network extender 110 using the communication link 123.

DEPR:
At a step 254, the network extender 110 receives the LEX protocol wrapper 210 using the communication link 123. The network extender 110 detects the LEX header 211 and separates the LEX header 211 from the LEX body 212.

DEPR:
At a step 255, the network extender 110 interprets the LEX header 211, which designates the LEX body 212 as intended for redistribution onto the network 101 (that is, a network packet 200), or as intended as a control message designated for the network extender 110 itself. If the LEX body 212 is a network packet 200, the network extender 110 proceeds to the step 256. Otherwise, the network extender 110 proceeds to the step 257.

DEPR:
At a step 256, the network extender 110 unwraps the LEX header 211 from the LEX protocol wrapper 210, and redistributes the LEX body 212 as a network packet 200 onto the network 101 using the network interface 104. The network's communication medium 102 transmits the network packet 200 to its destination device 103 (or devices 103, for example if the network packet 200 is a broadcast packet).

DEPR:
At a step 257, the network extender 110 unwraps the LEX header 211 from the LEX protocol wrapper 210, and interprets the LEX body 212 as a control message.

DEPR:
The following set of control messages comprises a set for a network extender 110 coupled to an ethernet LAN and operating according to an ethernet LAN protocol. In alternative embodiments, or with alternative network extenders 110 coupled to alternative networks 101, there might be a different set of control messages, or no control messages. For example, when the physical controller 132 is coupled to a PCMCIA card 150, there might be no control messages implemented at all.

DEPR:
A first control message comprises a negotiation control message for directing the network extender 110 to negotiate a set of parameters for establishing the communication link 123. The negotiation control message comprises a protocol version value, indicating the version of the LEX protocol supported by the router 120. The network extender 110 receives the protocol version value and responds with a negotiation control message indicating the version of the LEX protocol it supports. The router 120 and the network extender 110 each adjust their treatment of the communication link 123 to use the lower-numbered version of the LEX protocol.

DEPR:
A second control message comprises a protocol filtering control message for directing the network extender 110 to filter network packets 200 for those packets it should forward to the router 120 and those packets it should not forward. The protocol filtering control message comprises a sequence of tuples 213, in a canonical order, each tuple 213 comprising a protocol type 214 and a permit/deny bit 215 indicating whether a network packet 200 having that protocol type 214 should be forwarded or discarded. The sequence of tuples 213 is preceded by a sequence length field; a zero length sequence of tuples 213 is interpreted by the network extender 110 as a command to turn protocol filtering off.

DEPR:
A third control message comprises a destination filtering control

message for directing the network extender 110 to filter network packets 200, similar to the protocol filtering control message. The destination filtering control message comprises a sequence of tuples 213, in a canonical order, each tuple 213 comprising a destination address 216 and a permit/deny bit 215 indicating whether a network packet 200 having that protocol type 214 should be forwarded or discarded. The sequence of tuples 213 is preceded by a sequence length field; a zero length sequence of tuples 213 is interpreted by the network extender 110 as a command to turn destination filtering off.

DEPR:
The network extender 110 parses the filtering control message and the destination filtering control message, and in response constructs a trie 217 embodying the instructions in the sequence of tuples 213 of protocol types 214 and permit/deny bits 215 or tuples 213 of destination addresses 216 and permit/deny bits 215. When the network extender 110 receives a network packet 200, as at the step 262, it matches the protocol type 215 and destination address 216 of the network packet 200 against the trie 217 to determine whether it should forward or discard the network packet 200.

DEPR:
In a preferred embodiment, the router 120 already comprises means for filtering packets 200 for those packets 200 it should forward to the network 101 and those packets 200 it should not forward, and does not generally require filtering information from the network extender 110.

DEPR:
A fourth control message comprises a priority queuing control message for directing the network extender 110 to prioritizing packets 200 to be queued for transmission to the router 120 using the communication link 123. The priority queuing control message comprises a sequence of tuples 213, in a canonical order, each tuple 213 comprising a protocol type 214 and a priority value 218 indicating what priority value to assign a network packet 200 having that protocol type 214. The sequence of tuples 213 is preceded by a sequence length field; a zero length sequence of tuples 213 is interpreted by the network extender 110 as a command to assign all packets the same priority value.

DEPR:
A fifth control message comprises a report statistics control message for directing the network extender 110 to respond with a report of operational statistics. The report statistics control message comprises a set of statistics flags, directing which statistics to report and directing the network extender 110 whether to reset those statistics upon reporting them.

DEPR:
In a preferred embodiment, the statistics flags comprise a first flag directing the network extender 110 to resent statistics after reporting, a second flag directing the network extender 110 to report statistics regarding the communication link 123, and a third flag directing the network extender 110 to report statistics regarding the network's communication medium 102. Statistics to be reported may comprise numbers of packets transmitted or received, errors of various types, latency times, transmission rates for packets or data, and other statistics known in the art of computer networking.

DEPR:
A sixth control message comprises a reboot control message for directing the network extender 110 to reboot itself.

DEPR:
A seventh control message comprises a download control message for directing the network extender 110 to download data comprising a program, a set of options, or other data.

DEPR:
An eighth control message comprises a download status control message for directing the network extender 110 to report status of a recent download control message.

DEPR:
A ninth control message comprises a disable network control message for directing the network extender 110 to disable its connectivity to the network 101.

DEPR:
A tenth control message comprises an enable network control message for directing the network extender 110 to enable its connectivity to the network 101.

DEPR:
An eleventh control message comprises an inventory control message for directing the network extender 110 to respond with a report of its hardware and software, including version numbers.

DEPR:
At a step 262, the network extender 110 receives the network packet 200 using the network's communication medium 102. The network extender 110 detects the packet header 201 and determines whether the destination address is one it should forward to the router 120. If the destination address is one it should forward, the network extender 110 proceeds to the step 263. Otherwise, the network extender 110 discards the packet 200.

DEPR:
At a step 263, the network extender 110 attempt to make a communication link 123 with the router 120. If the network extender 110 already has a communication link 123 is progress with the router 120, the network extender 110 proceeds to the step 264. Otherwise, the network extender 110 establishes the communication link 123 with the router 120 using the telephone network 113. Establishing communication links using a telephone network is known in the art of computer communication.

DEPR:
At a step 264, the router 120 receives the incoming communication link 123 to the router's serial port 121. The router 120 negotiates with the network extender 110 to establish the communication link 123 with acceptable parameters (for example, line speed), using a negotiation control message described with the step 257. Negotiation to establish link parameters is known in the art of computer communication.

DEPR:
At a step 265, the network extender 110 transmits authentication information to the router 120 using the communication link 123. In a preferred embodiment, the authentication information is a MAC address for the network extender 110.

DEPR:
At a step 266, the router 120 receives the authentication/identification information and attempts to authenticate the network extender 110. If the router 120 is able to authenticate the network extender 110, it proceeds to the step 267. Otherwise, the router 120 so informs the network extender 110 and breaks the communication link 123.

DEPR:
In alternative embodiments, the step 265 and the step 266 may comprise a more elaborate or secure method of identification and authentication, such as PPP CHAP. For example, the step 266 may comprise a distinct authentication technique, and may comprise the exchange of information between the network extender 110 and the

router 120 using the communication link 123. In such alternative embodiments, the router 120 attempts to identify and authenticate the network extender 110 before binding the virtual controller to the physical controller for the communication link 123 in the step 267.

DEPR:
At a step 267, the router 120 searches a lookup table for the virtual controller 134 associated with the network extender 110, and binds that virtual controller 134 to the physical controller 132 for the communication link 123. In a preferred embodiment, the MAC address for the network extender is associated with a single virtual controller 134. If no such virtual controller 134 exists (that is, the type of virtual port 135 is known but there is no instantiation of the virtual controller 134 for this particular network extender 110), the router 120 creates an instantiation of the associated virtual controller 134 and assigns that virtual controller 134 parameters for the communication link 123.

DEPR:
At a step 268, the network extender 110 wraps the network packet 200 in the LEX protocol wrapper 210, comprising a LEX header 211 and a LEX body 212, and transmits the LEX protocol wrapper 210 to the router 120 using the communication link 123. The LEX body 212 comprises the network packet 200.

DEPR:
The network extender 110 is also disposed to send a LEX protocol wrapper 210 comprising a LEX header 211 and a LEX body 212, where the LEX body 212 is a control message to the router 120 or a response to a control message from the router 120. When the LEX body 212 is a control message or a response to a control message, the router 120 detects this and does not forward the LEX body 212 onto the second network 124.

DEPL:
The Network Extender

CLPR:
5. A system as in claim 1, wherein said network extender further comprises

CLPV:
a network extender having a serial port and disposed for controlling the network extender's serial port, and operatively coupled to said network interface; and

CLPV:
an application disposed to supply administrative services to the network when said router is coupled to said network extender, wherein said virtual controller is disposed to couple said application to said emulated port.

CLPV:
means for coupling said device to a first computer network and for transmitting said administrative control message to said network extender and

CLPV:
a first network extender having a serial port and disposed for controlling said first network extender's serial port, and operatively coupled to said first network interface;

CLPV:
a second network extender having a serial port and disposed for controlling said second network extender's serial port, and operatively coupled to said second network interface; and means for establishing a binding between said physical interface controller and either said first or second virtual interface controller.

Document Number 3

Entry 3 of 4 File: USPT Aug 18, 1998

DOCUMENT-IDENTIFIER: US 5796742 A
TITLE: Bi-diredctional wire-line to local area network interface and method

DEPR:
Consider data originating on the remote host 17 and propagating via the local area network 10 through the module to the wire-line carrier system 16. The remote host 17 sends data over the physical Ethernet medium of the local area network 10 which is demodulated by the cable transceiver 31, decoded by the Encoder/Decoder (ENDEC) module 32 which converts the Manchester encoded information to binary information and sends it to the Media Access Control (MAC) layer 33. The MAC layer 33 contains an integral controller which now converts the binary information to a machine-readable format and controls its movement to the link layer control (LLC) module 34. The LLC 34 is responsible for identification of the incoming data packet by its protocol type. The wire-line carrier to LAN module recognizes two types of packets at this layer: (i) Internet Protocol (IP) and (iii) Address Resolution Protocol (ARP). The LLC module 34 discards all other types of data, if any, arriving from the MAC layer 33. In the case of information having the packet type IP, then the LLC module 34 sends the incoming packet to the internet protocol module 36. At this layer, there are two possible destinations for the IP packet: (i) internet control message protocol (ICMP) 37 or (ii) transmission control protocol (TCP) 38. In the case of a TCP packet, the internet protocol module 36 sends the packet to the TCP module 38 which may either request that the remote host 17 send another packet if the data or headers were mangled, or send the packet to Telnet 39 for correlation to its bi-directional session. Telnet 39 then sends the packet to a command packet recognition module 41 which may find that the packet comprises a modem control command, which is decoded and sent to the wire-line carrier connection controller 47. In the case that the command recognition module 41 finds that the packet arriving is not a modem command, then it is presumed to be treated as "data", which is correlated to its wire-line carrier channel number 41 by reference to its session number and de-packetized 43 into binary data and sent to the wire-line carrier call controller and second signal transform 48. The data depacketizer's queues 42 are polled round-robin by the second signal transform 48. Data are dequeued one character at a time. The channel number is received from the session number correlation module 42. The character is encoded with the appropriate error detection and correction bits. The characters are collected and data compression techniques are applied. Error detection/correction and data compression methods are negotiated at call connection time. The data are then transformed directly from binary to a digitized representation of an analog signal, based on the modulation scheme employed, in the form of PCM octets. Several octets make up one signal. The octets are sent to the multiplexer 49 along with the channel on which they are to be transmitted. Octet data samples from each active channel are sent from second signal transform 48 every 125 microseconds to the multiplexer 49 where frame bits, wire-line carrier alarm conditions and signaling bits, e.g. on/off hook, are combined to build a wire-line carrier signal, e.g., a DS1 signal. The wire-line carrier signal is delivered to the wire-line carrier transmit side.

extender

What is extender?

WEST

Help | Logout

Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers

Search Results -

Terms	Documents
5867666 [pn] and extender	1

Database: US Patents Full-Text Database

Refine Search: 5867666 [pn] and extender

Search History

DB Name	Query	Hit Count	Set Name
USPT	5867666 [pn] and extender	1	L13
USPT	l11 same (depacket$ or de adj packet$ or deencapsulat$ or de adj encapsulat$ or unwrap$)	4	L12
USPT	l8 same (access$ or filter$)	44	L11
USPT	l8 same (lec)	1	L10
USPT	l8 same (lex)	1	L9
USPT	l7 same (filter$ or compar$ or bit$1 or field$1 or list or access or database)	134	L8
USPT	l5 same (extender or form$ or build$ or generat$ or packet$ or creat$ wrap$)	209	L7
USPT	l5 same (form$ or build$ or generat$ or packet$ or creat$ wrap$)	209	L6
USPT	l4 same (destination or address or network or rout$ or gateway or device)	253	L5
USPT	l2 same (wrapper or protocol or encapsulat$ or envelop$)	322	L4
USPT	l2 same (wrapper)	1	L3
USPT	l1 same (header or body)	1622	L2
USPT	(packet or frame) same (lex or lec or exchange or local)	17081	L1